Status:	**Active Policy**
Effective Date:	October 10, 2007 through October 9, 2009
Revised Date:	N/A
Approved By:	J. Stephen Fletcher, CIO
Authority:	*UCA §63F-1-206; Utah Administrative Code, R895-7. Acceptable Use of Information Technology Resources; Governor's Executive Order: Directing the Chief Information Officer to Develop and Implement Policy Promoting Security of State Information and Information Systems; DTS Policy and Procedure 1000-0003 Acceptable Use of Information Technology Resources*

1700.1 PURPOSE

To establish a policy that clarifies the need for employees and contractors to be aware that information is to be protected.

1700.1.1 Background

On December 11, 2001, the Governor of Utah issued an executive order directing the Chief Information Officer (CIO) to develop and implement policies that promote the security of state information and information systems. The CIO has determined that information security is an issue for all state agencies, and the Department of Technology Services (DTS) will assist agencies to govern and protect their information assets.

DTS will develop and implement security controls based on business rules which govern access and provide sufficient protection for each information asset. DTS will safeguard information assets through the application and enforcement of security controls which reduce the risk of accidental or intentional removal of data.

1700.1.2 Scope

This policy applies to all employees and contractors within the Department of Technology Services (DTS).

1700.1.3 Exceptions

Agencies excluded under the provisions of *§63F-1-102 (7) et seq.,* are not included under the provisions of this policy.

The CIO may grant a policy exception to an Executive Branch Agency when the requesting agency's Executive Director/Commissioner, or their designee, and the CIO determine that compliance would be overly burdensome and/or detrimental to the mission of the state. All exceptions must be approved in writing by the CIO.

1700.2 DEFINITIONS

Asset Owner
An entity recognized or identified by the State of Utah as an actual or potential owner of real, personal, or intellectual property. For the purposes of this policy, the Asset Owner of DTS property is the CIO.

Confidential Information
For the purposes of this policy, Confidential Information includes, but is not limited to, financial, health, social-security, criminal, biometric, or any other personally identifiable information which, if inappropriately disclosed, could lead to a significant negative impact on the subject. Confidential Information may also include information designated as confidential, private, controlled or any other equivalent term within statute, rule, policy or regulation.

Employee
For the purposes of this policy an employee is any individual employed by the Department or any individual who provides IT services and/or performs IT tasks for the Department in accordance with a contractual agreement (i.e., a contractor).

Information Asset
Information that is prepared, owned, received, or retained by an entity that in its original form is reproducible by mechanical or electronic means.

Information Technology Device
For the purposes of this policy the term information technology device includes, but is not limited to, any equipment or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of information.

1700.3 POLICY

Access to, disclosure or modification of, an information asset within the control of DTS must be authorized by the asset owner. Any and all information assets shall not be disclosed or provided, in any form, to unauthorized recipients.

All DTS employees, at the time of hire, must sign a Confidentiality Agreement. Annually DTS employees must review the current Data Confidentiality Policy and acknowledge they have read and understand it. All contractors hired by DTS that have access to information assets must sign a confidentiality agreement before service execution.

1700.3.1 General

1700.3.1.1 Employees and contractors shall become familiar with and comply with all relevant Department security policies, including but not limited to, this policy, UAC R895-1 Access of Records, the DTS Code of Conduct, and other policies, rules, and statutes related to data protection, information use and privacy rights.

1700.3.1.2 Employees and contractors shall ensure that information assets are protected at all times through the judicious use of readily available data protection tools (e.g., passwords, data encryption, discretionary access controls), and ensuring that minimal access to information assets is enforced at all times.

1700.3.1.3 Employees and contractors shall ensure that confidential information, stored on any state, local, or federal production and/or development system, is treated in a confidential manner and protected appropriately, including actively safeguarding and supporting the security needs of each system.

1700.3.1.4 Employees and contractors with access to information should understand the need to protect it, enforce safeguards that ensure confidential information may only be accessed during the course of normal business processes, and understand their responsibility for ensuring that information assets are always protected.

1700.3.1.5 Employees and contractors shall ensure that when an information asset is no longer required, any information extracted or copied from an electronic resource is disposed of in a manner that safeguards against unauthorized interception. Generally, paper-based duplicate copies shall be properly shredded and electronic data or data facsimiles shall be destroyed.

1700.3.2 Inspection of Information Technology Devices

To assure compliance with DTS policy and state and federal laws DTS has the right to inspect any and all information technology devices that are or have been connected to the state's secured information technology system (e.g., WAN). Employees who do not wish such inspections to be done on their personal information technology device or imaging device should not bring such items to work at all.

Employees and contractors should not bring personal or non-state owned information technology equipment to the workplace or connect them to the state's secured information technology systems unless expressly permitted to do so by DTS.

Employees and contractors observed bringing personal or non-state owned information technology equipment onto Department premises shall be provided the following notice: "Any information technology device, including an image recording device, brought onto Department premises may be subject to inspection by Department of Technology Services personnel at any time. Device inspection may include a detailed review of any file, information asset, or data storage media installed or connected to the information technology device in question." The aforementioned notice may be provided verbally, delivered via an automated information technology process, or posted in a format that is recognizable and readable to the average person as long as the notice is displayed in a conspicuous

location.

1700.3.3 Protection of Information

In the course of performing assigned tasks access to information assets may be necessary. No information assets which identify specific individuals or other personally identifiable information may be accessed by any party unless required during the normal performance of duties.

1700.3.3.1 Without written permission of the information asset owner confidential information assets may not be disclosed or distributed to unauthorized individuals or entities.

1700.3.3.2 Without written permission of the information asset owner, no aggregate information from information asset records shall be reported, published, or distributed.

1700.3.3.3 Without written permission of the information asset owner, information assets may not be copied, stored, or distributed in any format, or for any intent, outside of approved processing and troubleshooting methods.

1700.3.3.4 Without written permission of the information asset owner, developers may not copy information assets for development and testing purposes. Authority to copy information assets may be obtained on a single event basis, a project basis, or a time-specific basis.

1700.3.3.5 Without written permission of the information asset owner or the CIO, and utilizing appropriate protection measures, information assets classified as confidential may not be:

- Copied to removable media devices such as, but not limited to, tape, USB drives, CD-ROM, DVD, and PDAs (See also 1700.3.3.5.1)
- Transmitted over unsecured and/or unencrypted networks
- Sent via unencrypted email
- Transmitted via unencrypted File Transfer Protocol (FTP)

1700.3.3.5.1 When copied as part of a DTS approved data backup and storage process information assets may be copied to removable media without written permission.

1700.3.3.5.2 Appropriate protection measures shall be defined, reviewed, and made available for use within the Department by the Enterprise Information Security Office.

1700.3.4 Release of Information

Employees and contractors shall ensure that information assets are protected at all times. The Department may take action, up to and including all State and Federal

sanctions, against employees and contractors whose failure to adequately protect information assets results in an unauthorized release of confidential information.

1700.3.4.1 Any unauthorized release or security breach of confidential information shall be reported immediately to the employee's supervisor. DTS Supervisors are obligated to notify the CIO or Chief Information Security Officer (CISO) of any reported or suspected security breaches.

1700.3.4.2 A mechanism will be established for the anonymous reporting of data security breaches. Any employee or contractor who believes that a data security breach has occurred and wishing to remain anonymous may report the incident using this method.

1700.3.5 Removal of Information

Upon the request of or termination from the Department, employees and contractors shall deliver to the Department any documents and materials received or originating from its activities for the Department. Employees and contractors shall remove all confidential information from their information technology devices and permit the Department to inspect their information technology device(s) to ensure all confidential information has been removed and is no longer recoverable.

1700.4 ENFORCEMENT

Violation of this policy may be the basis for discipline including but not limited to termination. Individuals found to have violated this policy may also be subject to legal penalties as may be prescribed by state and/or federal statute, rule, and/or regulation.

1700.4 APPENDICES

- Data Confidentiality Agreement
- Data Confidentially FAQs

DOCUMENT HISTORY

Originator:	Michael Casey, Chief Information Security Officer
Next Review:	August 20, 2009
Reviewed Date:	N/A
Reviewed By:	N/A